CSIOS Corporation

https://www.csioscorp.com

257 Mohegan Dr, Havre De Grace, Maryland 21078

DUNS: 079858391

General Services Administration Federal Supply Service
GSA Multiple Award Schedule (MAS)

GSA Schedule Contract Administration:

Name: Mr. Cesar Pie

Phone: (301) 752–2729

Contract Number: GS–35F–657GA

Modification: PA-0013 dated October 22, 2021

Contract Period: September 6, 2017 through September 5, 2022

54151HACS	*Highly Adaptive Cybersecurity Services (HACS)*
54151S	*Information Technology Professional Services*

TABLE OF CONTENTS

CSIOS CORPORATION

CSIOS Corporation is an **ISO 9001** (*Quality Management System*), **ISO/IEC 20000** (*Information Technology Service Management*), **ISO 22301** (*Business Continuity Management Systems*), and **ISO/IEC 27001** (*Information Security Management Systems*) compliant and certified **Veteran–Owned Small Business** provider of **Cyberspace** and **Information Network Operations**, **Cybersecurity**, and **Information Technology** services.

I–FSS–600 CONTRACT PRICE LISTSGENERAL SERVICES ADMINISTRATION

Federal Supply Service

Authorized Federal Supply Schedule Price List

On–line access to contract ordering information, terms and conditions, up–to– date pricing, and the option to create an electronic delivery order are available through GSA Advantage! a menu–driven database system. The INTERNET address for GSA Advantage! is: GSAAdvantage.gov.

Schedule Title: Multiple Award Schedule

FSC Group, Part, and Section or Standard Industrial Group (as applicable): Information Technology

FSC Class(es)/Product code(s) and/or Service Codes (as applicable): 54151HACS – DJ01; 54151S – DA01,

Contract number: **GS–35F–657GA**

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.

Contract period: **September 6, 2017 through September 5, 2022**

Contractor's name, address, and phone number (include toll–free WATS number and FAX number, if applicable):

CSIOS Corporation

257 Mohegan Dr, Havre De Grace, Maryland 21078

Tel: (301) 752–2729

Contractor's internet address/web site where schedule information can be found (as applicable): www.csioscorp.com

Contract administration source (if different from preceding entry):

Mr. Cesar Pie

Cesar.Pie@csioscorp.com

Tel: (301) 752–2729

Business size: **Small**

CUSTOMER INFORMATION: The following information should be placed under this heading in consecutively numbered paragraphs in the sequence set forth below. If this information is placed in another part of the Federal Supply Schedule Price List, a table of contents must be shown on the cover page that refers to the exact location of the information.

1a. Table of awarded special item number(s) with appropriate cross– reference to item descriptions and awarded price(s): **SINs 54151HACS, 54151S**

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

See attached CSIOS GSA Price List.

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate "Not applicable" for this item. See attached CSIOS GSA Price List.

2. Maximum order: **54151HACS – $500,000; 54151S– $500,000**

3. Minimum order: **$100.00**

4. Geographic coverage (delivery area): **Worldwide**

5. Point(s) of production (city, county, and State or foreign country): **N/A**

6. Discount from list, prices or statement of net price: **10% to Federal Government**

7. Quantity discounts: **1% on orders over $500,000**

8. Prompt payment terms: **1% 20 days, NET 30**

9a. Notification that Government purchase cards are accepted at or below the micro–purchase threshold: **Government purchase cards are accepted in full**

9b. Notification whether Government purchase cards are accepted or not accepted above the micro–purchase threshold: **Government purchase cards are accepted**

10. Foreign items (list items by country of origin): **N/A**

11a. Time of delivery: **N.A**

l1b. Expedited Delivery. The Contractor will insert the sentence "Items available for expedited delivery are noted in this price list." Under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery: **N/A**

l1c. Overnight and 2–day delivery. The Contractor will indicate whether overnight and 2–day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2–day delivery: **N/A**

11d. Urgent Requirements. The Contractor will note in its price list the Urgent. Requirements" clause of its contract and advice agencies that they can also contact the Contractor's representative to affect a faster delivery.

12. F.O.B. point(s): **N/A**

13a. Ordering address(es): **N/A**

13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs), and a sample EPA can be found at the

GSA/FSS Schedule homepage (fss.gsa.gov/schedules). Contactor is to simply include this statement as item 13b.

14. Payment address(es):

CSIOS Corporation

451 Hungerford Drive, Suite 119–358,

Rockville, MD 20850

15. Warranty provision: **N/A**

16. Export packing charges, if applicable: **N/A**

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro–purchase level): **N/A**

18. Terms and conditions of rental, maintenance, and repair (if applicable): **N/A**

19. Terms and conditions of installation (if applicable): **N/A**

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): **N/A**

20a. Terms and conditions for any other services (if applicable): **N/A**

21. List of service and distribution points (if applicable): **N/A**

22. List of participating dealers (if applicab1e): **N/A**

23. Preventive maintenance (if applicable): **N/A**

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): **N/A**

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contractor's website or other location.) The EIT standards can he found at www.Section508.gov/: **N/A**

25. Data Universal Number System (DUNS) number: **079858391**

26. Notification regarding registration in SAM Registration database:

CSIOS Corporation SAM registration is valid through 01/04/2022.

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (54151HACS)

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204–21
- OMB Memorandum M–06–19 – Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M –07–16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M–16–03 – Fiscal Year 2015–2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M–16–04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800–14 – Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800–27A – Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800–30 – Guide for Conducting Risk Assessments
- NIST SP 800–35 – Guide to Information Technology Security Services
- NIST SP 800–37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST SP 800–39 – Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800–44 – Guidelines on Securing Public Web Servers
- NIST SP 800–48 – Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800–53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800–61 – Computer Security Incident Handling Guide
- NIST SP 800–64 – Security Considerations in the System Development Life Cycle
- NIST SP 800–82 – Guide to Industrial Control Systems (ICS) Security
- NIST SP 800–86 – Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800–115 – Technical Guide to Information Security Testing and Assessment
- NIST SP 800–128 – Guide for Security–Focused Configuration Management of Information Systems
- NIST SP 800–137 – Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800–153 – Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800–171 – Protecting Controlled Unclassified Information in non–federal Information Systems and Organizations

1. SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Multiple Award Schedule.
b. The five (5) subcategories for services under the HACS SIN: High Value Asset (HVA) Assessments; Risk and Vulnerability Assessment; Cyber Hunt; Incident Response; and Penetration Testing
c. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on – Multiple Award Schedule (e.g. 511210, 33411), and may be quoted along with services to provide a total solution.
d. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
e. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
f. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. ORDER

a. Agencies may use written orders, Electronic Data Interchange (EDI) orders, Blanket Purchase Agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232–19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

3. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use

GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212–4 – CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm–Fixed Price and Time–and–Materials and Labor–Hour Contracts orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227–14 (MAY 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204–21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to the ordering activity's security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

7. INDEPENDENT CONTRACTOR

All Highly Adaptive Cybersecurity Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

- "Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
- "Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
- An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

10. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004)

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SIN 54151S)

1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT/IAM Professional Services within the scope of this Multiple Award Schedule.
b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I–FSS–60 PERFORMANCE INCENTIVES (APRIL 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232–19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any Contractor travel required in the performance of IT/IAM Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the

date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP–WORK ORDER (FAR 52.242–15) (AUG 1989)

a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop–work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop–work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either– (1) Cancel the stop–work order; or (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

b. If a stop–work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if–(1) The stop–work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

c. If a stop–work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop–work order in arriving at the termination settlement.

d. If a stop–work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop–work order.

6. INSPECTION OF SERVICES

In accordance with FAR 52.212–4 CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS (MAR 2009) (DEVIATION I – FEB 2007) for Firm–Fixed Price orders and FAR 52.212–4 CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I OCT 2008) (DEVIATION I – FEB 2007) applies to Time–and–Materials and Labor–Hour Contracts orders placed under this contract.

7. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227–14 (Dec 2007) Rights in Data – General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/IAM Professional Services.

9. INDEPENDENT CONTRACTOR

All IT/IAM Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

- "Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
- "Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
- An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

a. Delivery Terms: 30 days ARO or as negotiated with agency
b. Expedited Delivery Terms: Negotiated with customer

12. PAYMENTS

FOB Shipping Terms: Destination.

For firm–fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time–and–materials orders, the Payments under Time–and–Materials and Labor–Hour Contracts at FAR 52.212–4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time–and–materials orders placed under this contract. For labor–hour orders, the Payment under Time–and–Materials and Labor–Hour Contracts at FAR 52.212–4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor–hour orders placed under this contract. 52.216–31(Feb 2007) Time–and Materials/Labor–Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

a. The Government contemplates award of a Time–and–Materials or Labor–Hour type of contract resulting from this solicitation.
b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by— (1) The offeror; (2) Subcontractors; and/or (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. DESCRIPTION OF IT SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151HACS and 54151S. IT Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
b. Pricing for all IT Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.

LABOR CATEGORY PRICE LIST

Labor Rates are for Contractor and/or Customer Facility

SIN(S) PROPOSED	ID/LABOR CATEGORY TITLE	GSA PRICE (INCLUDING IFF)
54151S	Cloud Computing Engineer, Level I	$93.28
54151S	Cloud Computing Engineer, Level II	$105.40
54151S	Cloud Computing Engineer, Level III	$117.51
54151S	Cloud Computing Engineer, Level IV	$129.64
54151S	Cloud Computing Engineer, Level V	$141.74
54151S	Cloud Computing Engineer, Subject Matter Expert I	$153.87
54151S	Cloud Computing Engineer, Subject Matter Expert II	$165.98
54151S	Cloud Computing Engineer, Subject Matter Expert III	$178.10
54151S	Cloud Computing Cybersecurity Specialist, Level I	$94.74
54151S	Cloud Computing Cybersecurity Specialist, Level II	$106.86
54151S	Cloud Computing Cybersecurity Specialist, Level III	$118.98
54151S	Cloud Computing Cybersecurity Specialist, Level IV	$131.10
54151S	Cloud Computing Cybersecurity Specialist, Level V	$143.21
54151S	Cloud Computing Cybersecurity Operations, Subject Matter Expert I	$155.33
54151S	Cloud Computing Cybersecurity Operations, Subject Matter Expert II	$167.45
54151S	Cloud Computing Cybersecurity Operations, Subject Matter Expert III	$179.56
54151HACS	Cybersecurity Consultant, Level I	$89.95
54151HACS	Cybersecurity Consultant, Level II	$105.09
54151HACS	Cybersecurity Consultant, Level III	$120.25
54151HACS	Cybersecurity Consultant, Level IV	$135.39
54151HACS	Cybersecurity Consultant, Level V	$150.53
54151HACS	Cybersecurity Consultant, Subject Matter Expert I	$165.68
54151HACS	Cybersecurity Consultant, Subject Matter Expert II	$180.83
54151HACS	Cybersecurity Consultant, Subject Matter Expert III	$195.99
54151HACS	Cyberspace Operations Analyst, Level I	$88.97

54151HACS	Cyberspace Operations Analyst, Level II	$105.11
54151HACS	Cyberspace Operations Analyst, Level III	$121.26
54151HACS	Cyberspace Operations Analyst, Level IV	$137.41
54151HACS	Cyberspace Operations Analyst, Level V	$153.55
54151HACS	Cyberspace Operations, Subject Matter Expert I	$169.69
54151HACS	Cyberspace Operations, Subject Matter Expert II	$185.84
54151HACS	Cyberspace Operations, Subject Matter Expert III	$201.98
54151HACS	Cyberspace Operations, Manager	$208.05
54151HACS	Cyberspace Operations, Sr. Manager	$214.29
54151HACS	Cyberspace Operations, Director	$220.72
54151HACS	Cyber Research and Development, Level I	$80.08
54151HACS	Cyber Research and Development, Level II	$90.04
54151HACS	Cyber Research and Development, Level III	$106.17
54151HACS	Cyber Research and Development, Level IV	$122.32
54151HACS	Cyber Research and Development, Level V	$138.47
54151HACS	Cyber Research and Development, Subject Matter Expert I	$154.62
54151HACS	Cyber Research and Development, Subject Matter Expert II	$170.76
54151HACS	Cyber Research and Development, Subject Matter Expert III	$186.91
54151HACS	Cyber Strategist, Level I	$83.05
54151HACS	Cyber Strategist, Level II	$93.42
54151HACS	Cyber Strategist, Level III	$109.58
54151HACS	Cyber Strategist, Level IV	$125.71
54151HACS	Cyber Strategist, Level V	$141.86
54151HACS	Cyber Strategist, Subject Matter Expert I	$158.00
54151HACS	Cyber Strategist, Subject Matter Expert II	$174.15
54151HACS	Cyber Strategist, Subject Matter Expert III	$190.29
54151HACS	Cyber Test and Evaluation, Level I	$80.70
54151HACS	Cyber Test and Evaluation, Level II	$92.88
54151HACS	Cyber Test and Evaluation, Level III	$105.07

54151HACS	Cyber Test and Evaluation, Level IV	$117.26
54151HACS	Cyber Test and Evaluation, Level V	$129.45
54151HACS	Cyber Test and Evaluation, Subject Matter Expert I	$141.62
54151HACS	Cyber Test and Evaluation, Subject Matter Expert II	$153.82
54151HACS	Cyber Test and Evaluation, Subject Matter Expert III	$166.00
54151HACS	Cyber Threat Analyst, Level I	$90.65
54151HACS	Cyber Threat Analyst, Level II	$105.81
54151HACS	Cyber Threat Analyst, Level III	$120.96
54151HACS	Cyber Threat Analyst, Level IV	$136.09
54151HACS	Cyber Threat Analyst, Level V	$151.25
54151HACS	Cyber Threat Analyst, Subject Matter Expert I	$166.40
54151HACS	Cyber Threat Analyst, Subject Matter Expert II	$181.54
54151HACS	Cyber Threat Analyst, Subject Matter Expert III	$196.69
54151HACS	Cyber Threat Analyst, Manager	$202.59
54151HACS	Cyber Threat Analyst, Sr. Manager	$208.67
54151HACS	Cyber Threat Analyst, Director	$214.93
54151HACS	Cybersecurity Training Specialist, Level I	$63.70
54151HACS	Cybersecurity Training Specialist, Level II	$77.93
54151HACS	Cybersecurity Training Specialist, Level III	$92.16
54151HACS	Cybersecurity Training Specialist, Level IV	$106.39
54151HACS	Cybersecurity Training Specialist, Level V	$120.62
54151HACS	Cybersecurity Training Specialist, Subject Matter Expert I	$134.86
54151HACS	Cybersecurity Training Specialist, Subject Matter Expert II	$149.09
54151HACS	Cybersecurity Training Specialist, Subject Matter Expert III	$163.31
54151HACS	Defensive Cyberspace Operations, Level I	$77.30
54151HACS	Defensive Cyberspace Operations, Level II	$93.45
54151HACS	Defensive Cyberspace Operations, Level III	$109.60
54151HACS	Defensive Cyberspace Operations, Level IV	$125.74
54151HACS	Defensive Cyberspace Operations, Level V	$141.90

54151HACS	Defensive Cyberspace Operations, Subject Matter Expert I	$158.03
54151HACS	Defensive Cyberspace Operations, Subject Matter Expert II	$174.18
54151HACS	Defensive Cyberspace Operations, Subject Matter Expert III	$190.32
54151HACS	Defensive Cyberspace Operations, Manager	$196.02
54151HACS	Defensive Cyberspace Operations, Sr. Manager	$201.91
54151HACS	Defensive Cyberspace Operations, Director	$207.97
54151S	Information Network Operations, Level I	$79.73
54151S	Information Network Operations, Level II	$95.88
54151S	Information Network Operations, Level III	$112.02
54151S	Information Network Operations, Level IV	$128.17
54151S	Information Network Operations, Level V	$144.32
54151S	Information Network Operations, Subject Matter Expert I	$160.47
54151S	Information Network Operations, Subject Matter Expert II	$176.61
54151S	Information Network Operations, Subject Matter Expert III	$192.75
54151S	Information Network Operations, Manager	$198.54
54151S	Information Network Operations, Sr. Manager	$204.48
54151S	Information Network Operations, Director	$210.63
54151HACS	Information Security Continuous Monitoring Analyst, Level I	$81.15
54151HACS	Information Security Continuous Monitoring Analyst, Level II	$95.23
54151HACS	Information Security Continuous Monitoring Analyst, Level III	$109.32
54151HACS	Information Security Continuous Monitoring Analyst, Level IV	$123.42
54151HACS	Information Security Continuous Monitoring Analyst, Level V	$137.52
54151HACS	Information Security Continuous Monitoring Analyst, Subject Matter Expert I	$151.60
54151HACS	Information Security Continuous Monitoring Analyst, Subject Matter Expert II	$165.69
54151HACS	Information Security Continuous Monitoring Analyst, Subject Matter Expert III	$179.78
54151HACS	Information Security Continuous Monitoring Engineer, Level I	$81.87
54151HACS	Information Security Continuous Monitoring Engineer, Level II	$96.88
54151HACS	Information Security Continuous Monitoring Engineer, Level III	$111.91

54151HACS	Information Security Continuous Monitoring Engineer, Level IV	$126.92
54151HACS	Information Security Continuous Monitoring Engineer, Level V	$141.94
54151HACS	Information Security Continuous Monitoring Engineer, Subject Matter Expert I	$156.98
54151HACS	Information Security Continuous Monitoring Engineer, Subject Matter Expert II	$171.98
54151HACS	Information Security Continuous Monitoring Engineer, Subject Matter Expert III	$187.01
54151S	Information Technologist, Level I	$79.19
54151S	Information Technologist, Level II	$94.14
54151S	Information Technologist, Level III	$109.10
54151S	Information Technologist, Level IV	$124.04
54151S	Information Technologist, Level V	$139.00
54151S	Information Technologist, Subject Matter Expert I	$153.94
54151S	Information Technologist, Subject Matter Expert II	$168.89
54151S	Information Technologist, Subject Matter Expert III	$183.84
54151S	Information Technologist, Manager	$189.36
54151S	Information Technologist, Sr. Manager	$195.03
54151S	Information Technologist, Director	$200.89
54151HACS	Offensive Cyberspace Operations, Level I	$80.61
54151HACS	Offensive Cyberspace Operations, Level II	$96.76
54151HACS	Offensive Cyberspace Operations, Level III	$112.90
54151HACS	Offensive Cyberspace Operations, Level IV	$129.06
54151HACS	Offensive Cyberspace Operations, Level V	$145.20
54151HACS	Offensive Cyberspace Operations, Subject Matter Expert I	$161.35
54151HACS	Offensive Cyberspace Operations, Subject Matter Expert II	$177.48
54151HACS	Offensive Cyberspace Operations, Subject Matter Expert III	$193.63
54151HACS	Offensive Cyberspace Operations, Manager	$199.43
54151HACS	Offensive Cyberspace Operations, Sr. Manager	$205.42
54151HACS	Offensive Cyberspace Operations, Director	$211.58
54151S	Project Manager, IT, Level I	$121.95
54151S	Project Manager, IT, Level II	$140.16

54151S	Project Manager, IT, Level III	$166.44
54151HACS	Project Manager, Cyber, Level I	$121.95
54151HACS	Project Manager, Cyber, Level II	$140.16
54151HACS	Project Manager, Cyber, Level III	$166.44
54151S	Program Manager, IT, Level I	$172.87
54151S	Program Manager, IT, Level II	$184.00
54151S	Program Manager, IT, Level III	$195.91
54151HACS	Program Manager, Cyber, Level I	$172.87
54151HACS	Program Manager, Cyber, Level II	$184.00
54151HACS	Program Manager, Cyber, Level III	$195.91
54151HACS	Risk and Vulnerability Analyst, Level I	$88.90
54151HACS	Risk and Vulnerability Analyst, Level II	$104.64
54151HACS	Risk and Vulnerability Analyst, Level III	$120.39
54151HACS	Risk and Vulnerability Analyst, Level IV	$136.14
54151HACS	Risk and Vulnerability Analyst, Level V	$151.87
54151HACS	Risk and Vulnerability Analyst, Subject Matter Expert I	$167.60
54151HACS	Risk and Vulnerability Analyst, Subject Matter Expert II	$183.36
54151HACS	Risk and Vulnerability Analyst, Subject Matter Expert III	$199.09
54151HACS	Risk and Vulnerability, Manager	$205.06
54151HACS	Risk and Vulnerability, Sr. Manager	$211.22
54151HACS	Risk and Vulnerability, Director	$217.56
54151HACS	Senior Analyst/Engineer, Level I	$103.07
54151HACS	Senior Analyst/Engineer, Level II	$120.64
54151HACS	Senior Analyst/Engineer, Level III	$134.53
54151HACS	Senior Analyst/Engineer, Level IV	$157.54
54151HACS	Senior Analyst/Engineer, Level V	$166.86
54151HACS	Subject Matter Expert I	$87.05
54151HACS	Subject Matter Expert II	$114.51
54151HACS	Subject Matter Expert III	$152.49

LABOR CATEGORY DESCRIPTIONS

CLOUD COMPUTING ENGINEER		
Applies cloud computing methods, tactics, tools, and techniques of engineering to conceive, develop, operate and maintain cloud computing systems and solutions. Applies technical and non–technical concepts, IT resources, and implementation mechanisms to engineer and evolve cloud platforms and models, such as Software–as–a–Service (SaaS), Platform–as–a–Service (PaaS), and Infrastructure–as–a–Service (IaaS). Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cloud Computing Engineer, Associate, Level I	High School Diploma and/or related and applicable IT certifications.	0–3
Cloud Computing Engineer, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable IT certifications.	3–6
Cloud Computing Engineer, Senior, Level III	Associate's degree in related discipline and/or related and applicable IT certifications.	6–10
Cloud Computing Engineer, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable IT certifications.	10
Cloud Computing Engineer, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable IT certifications.	12
Cloud Computing Engineer, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable IT certifications.	14
Cloud Computing Engineer, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable IT certifications.	16
Cloud Computing Engineer, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable IT certifications.	20

CLOUD COMPUTING CYBERSECURITY SPECIALIST		
Applies cloud computing methods, tactics, tools, and techniques to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, availability, authentication, and non–repudiation in cloud environments. Secures cloud platforms, infrastructures, and components, both physical and virtual, to include existing threats while mitigating and developing plans to deal with those threats. Identifies critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; the requirements of cloud architecture to run and manage that infrastructure; and security controls to manage and monitor risks and vulnerabilities. Ensures compliance with regulatory frameworks, privacy issues, and implications of cloud environments in relation to enterprise risk management. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cloud Computing Cybersecurity Specialist, Associate, Level I	High School Diploma and/or related and applicable IT certifications.	0–3
Cloud Computing Cybersecurity Specialist, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable IT certifications.	3–6
Cloud Computing Cybersecurity Specialist, Senior, Level III	Associate's degree in related discipline and/or related and applicable IT certifications.	6–10
Cloud Computing Cybersecurity Specialist, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable IT certifications.	10
Cloud Computing Cybersecurity Specialist, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable IT certifications.	12
Cloud Computing Cybersecurity Operations, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable IT certifications.	14
Cloud Computing Cybersecurity Operations, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable IT certifications.	16
Cloud Computing Cybersecurity Operations, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable IT certifications.	20

CYBERSECURITY CONSULTANT		
Works with technical, operational, and/or strategic groups to develop technical and non–technical solutions to protect and defend information systems and networks by ensuring their confidentiality, integrity, availability, authentication, and non–repudiation. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cybersecurity Consultant, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Cybersecurity Consultant, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cybersecurity Consultant, Senior, Level III	Associate's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cybersecurity Consultant, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cybersecurity Consultant, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cybersecurity Consultant, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cybersecurity Consultant, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cybersecurity Consultant, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBERSPACE OPERATIONS ANALYST		
Supports full spectrum cyberspace operations through the integrated and synchronized employment of offensive, defensive, and information network operations, underpinned by effective and timely technical and operational planning, preparation of the environment, execution, and evaluation. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cyberspace Operations Analyst, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Cyberspace Operations Analyst, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cyberspace Operations Analyst, Senior, Level III	Associate's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cyberspace Operations Analyst, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cyberspace Operations Analyst, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cyberspace Operations Analyst, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cyberspace Operations Analyst, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyberspace Operations Analyst, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20
Cyberspace Operations, Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	14
Cyberspace Operations, Sr. Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyberspace Operations, Director	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBER RESEARCH AND DEVELOPMENT		
Supports and fosters full spectrum research and development of transformative solutions to critical cyber security challenges, through partnerships with government, industry, and academia. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cyber Research and Development, Associate, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Cyber Research and Development, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cyber Research and Development, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cyber Research and Development, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cyber Research and Development, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cyber Research and Development, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cyber Research and Development, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyber Research and Development, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBER STRATEGIST		
Facilitates the development and maintenance life cycle of long– and short–term strategies, plans, and policies in support of cyberspace operations. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cyber Strategist, Associate, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Cyber Strategist, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cyber Strategist, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cyber Strategist, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cyber Strategist, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cyber Strategist, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cyber Strategist, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyber Strategist, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBER TEST AND EVALUATION		
Applies test and evaluation methods, tactics, tools, and techniques to methodically verify and validate compliance and measure the performance and effectiveness of technical and non–technical cybersecurity specifications, security controls, and requirements. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cyber Test and Evaluation, Associate, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Cyber Test and Evaluation, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cyber Test and Evaluation, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cyber Test and Evaluation, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cyber Test and Evaluation, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cyber Test and Evaluation, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cyber Test and Evaluation, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyber Test and Evaluation, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBER THREAT ANALYST		
Conducts all–source analysis, digital forensics, and targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber–related interests. Produces strategic assessments and provide tactical analysis and advice for cyber and intelligence operations. Applies scientific and technical knowledge to solve complex cyber and intelligence problems, produces short–term and long–term written assessments, and briefs decision makers to support organizational risk decision making. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cyber Threat Analyst, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Cyber Threat Analyst, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cyber Threat Analyst, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cyber Threat Analyst, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cyber Threat Analyst, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cyber Threat Analyst, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cyber Threat Analyst, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cyber Threat Analyst, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20
Cyber Threat Analyst, Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	14
Cyber Threat Analyst, Sr. Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	16

Cyber Threat Analyst, Director	Master's degree in related discipline and/or related and applicable cyber certifications.	20

CYBERSECURITY TRAINING SPECIALIST		
Develops, plans, coordinates, delivers, and/or evaluates instructional cybersecurity content using various training methods, tactics, tools, and techniques. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Cybersecurity Training Specialist, Associate, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Cybersecurity Training Specialist, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Cybersecurity Training Specialist, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Cybersecurity Training Specialist, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Cybersecurity Training Specialist, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Cybersecurity Training Specialist, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Cybersecurity Training Specialist, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Cybersecurity Training Specialist, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

DEFENSIVE CYBERSPACE OPERATIONS		
Supports activities to defend friendly cyberspace. Perform internal defensive measures to include actively hunting for advanced internal threats as well as the internal responses to these threats. Identifies, analyzes, and responds to unauthorized activity or alerts/threat information, and leverages intelligence, and other capabilities as required. Performs technical and non–technical activities and actions to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and networks. Supports full spectrum passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net–centric capabilities, and other designated systems. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Defensive Cyberspace Operations, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Defensive Cyberspace Operations, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Defensive Cyberspace Operations, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Defensive Cyberspace Operations, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Defensive Cyberspace Operations, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Defensive Cyberspace Operations, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Defensive Cyberspace Operations, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Defensive Cyberspace Operations, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20
Defensive Cyberspace Operations, Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	14
Defensive Cyberspace Operations, Sr. Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	16

Defensive Cyberspace Operations, Director	Master’s degree in related discipline and/or related and applicable cyber certifications.	20

INFORMATION NETWORK OPERATIONS		
Supports globally interconnected, end–to–end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on–demand to network defenders, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. Supports all the strategic, operational, technical, and tactical aspects needed to design, build, configure, secure, operate, maintain, and sustain information network operations while preserving cybersecurity. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Information Network Operations, Associate, Level I	High School Diploma and/or related and applicable IT certifications.	0–3
Information Network Operations, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable IT certifications.	3–6
Information Network Operations, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable IT certifications.	6–10
Information Network Operations, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable IT certifications.	10
Information Network Operations, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable IT certifications.	12
Information Network Operations, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable IT certifications.	14
Information Network Operations, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable IT certifications.	16
Information Network Operations, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable IT certifications.	20
Information Network Operations, Manager	Master's degree in related discipline and/or related and applicable IT certifications.	14
Information Network Operations, Sr. Manager	Master's degree in related discipline and/or related and applicable IT certifications.	16

Information Network Operations, Director	Master's degree in related discipline and/or related and applicable IT certifications.	20

INFORMATION SECURITY CONTINUOUS MONITORING ANALYST		
Provides on–going observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness. Supports strategic, operational, technical, and tactical activities to design, develop, install, implement, and test and evaluate an organization's information security continuous monitoring solutions and capabilities. Supports information security continuous monitoring integration activities and operational missions by providing tailored end–to–end services that provide measurable benefits, including greater efficiency and reduced costs and complexity. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Information Security Continuous Monitoring Analyst, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Information Security Continuous Monitoring Analyst, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Information Security Continuous Monitoring Analyst, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Information Security Continuous Monitoring Analyst, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Information Security Continuous Monitoring Analyst, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Information Security Continuous Monitoring Analyst, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Information Security Continuous Monitoring Analyst, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Information Security Continuous Monitoring Analyst, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

INFORMATION SECURITY CONTINUOUS MONITORING ENGINEER		
Applies engineering disciplines to information security continuous monitoring to include systematic approaches and solutions to concerns of commercialization, standardization, and governance of information security continuous monitoring applications, tools, and/or widgets. Applies information security continuous monitoring methods, tactics, tools, and techniques of engineering to conceive, develop, operate and maintain information security continuous monitoring solutions. Applies technical and non–technical concepts, IT resources, and implementation mechanisms to engineer and evolve an organization's information security continuous monitoring program. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Information Security Continuous Monitoring Engineer, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Information Security Continuous Monitoring Engineer, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Information Security Continuous Monitoring Engineer, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Information Security Continuous Monitoring Engineer, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Information Security Continuous Monitoring Engineer, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Information Security Continuous Monitoring Engineer, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Information Security Continuous Monitoring Engineer, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Information Security Continuous Monitoring Engineer, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

INFORMATION TECHNOLOGIST		
Performs technical assignments in the general area of command, control, communications, computers, combat systems, intelligence, surveillance, and reconnaissance (C5ISR). Applies information technology methods, tactics, tools, and techniques to evaluate, analyze, operate, maintain, manage, or improve C5ISR operating systems, applications, networks, databases, infrastructures, and other technical requirements. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Information Technologist, Associate, Level I	High School Diploma and/or related and applicable IT certifications.	0–3
Information Technologist, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable IT certifications.	3–6
Information Technologist, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable IT certifications.	6–10
Information Technologist, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable IT certifications.	10
Information Technologist, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable IT certifications.	12
Information Technologist, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable IT certifications.	14
Information Technologist, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable IT certifications.	16
Information Technologist, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable IT certifications.	20
Information Technologist, Manager	Master's degree in related discipline and/or related and applicable IT certifications.	14
Information Technologist, Sr. Manager	Master's degree in related discipline and/or related and applicable IT certifications.	16

Information Technologist, Director	Master's degree in related discipline and/or related and applicable IT certifications.	20

OFFENSIVE CYBERSPACE OPERATIONS		
Supports information gathering and operations in and through cyberspace. Participates in independent and focused threat–based efforts that simulate an interdisciplinary, simulated adversary to expose and exploit vulnerabilities as a means to improve the cybersecurity posture of information systems and networks. Supports exercise related activities, where the cyber operator simulates an opposing force and is focused on improving readiness and asses the performance of their people executing operations supported by their technology. Supports network penetration testing activities, where cyber operator provides security testing in an attempt to primarily circumvent the technology security features of a system based on their understanding of the system design and implementation. Supports all other authorized and organized activities to emulate a potential adversary's attack or exploitation capabilities with the intent to improve enterprise cybersecurity and cyberspace operations. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Offensive Cyberspace Operations, Associate, Level I	High School Diploma and/or related and applicable cyber certifications.	0–3
Offensive Cyberspace Operations, Intermediate, Level II	Associate's degree in related discipline and/or related and applicable cyber certifications.	3–6
Offensive Cyberspace Operations, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Offensive Cyberspace Operations, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Offensive Cyberspace Operations, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Offensive Cyberspace Operations, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Offensive Cyberspace Operations, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Offensive Cyberspace Operations, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

Offensive Cyberspace Operations, Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	14
Offensive Cyberspace Operations, Sr. Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Offensive Cyberspace Operations, Director	Master's degree in related discipline and/or related and applicable cyber certifications.	20

PROJECT MANAGER, IT		
Typically oversee all aspects of IT projects, leading a team on large projects or a significant segment of large and complex projects. Coordinate and collaborate with project stakeholders to ensure project plans, scope, goals, objectives, priorities, deliverables, milestones, and timelines are established and communicated. Analyze new and complex project–related problems and create innovative solutions that normally involve the schedule, technology, methodology, tools, solution components, and financial management of the project. Provide applications systems analysis and long and short–range plans for application selection, systems development, systems maintenance, and production activities for necessary support resources. Commensurate experience and education for the specific level. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Project Manager, IT, Level I	Associate's degree in related discipline and/or related and applicable IT certifications.	0–3
Project Manager, IT, Level II	Bachelor's degree in related discipline and/or related and applicable IT certifications.	3–6
Project Manager, IT, Level III	Bachelor's degree in related discipline and/or related and applicable IT certifications.	6–10

PROJECT MANAGER, CYBER		
Typically oversee all aspects of cyberspace operations project, leading a team on large projects or a significant segment of large and complex projects. Coordinate and collaborate with project stakeholders to ensure project plans, scope, goals, objectives, priorities, deliverables, milestones, and timelines are established and communicated. Analyze new and complex project–related problems and create innovative solutions that normally involve the schedule, technology, methodology, tools, solution components, and financial management of the project. Commensurate experience and education for the specific level. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Project Manager, Cyber, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	1
Project Manager, Cyber, Level II	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	3
Project Manager, Cyber, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6

PROGRAM MANAGER, IT		
Serves as the program manager typically responsible for organizing, directing, and managing all aspects of contract operational support functions involving multiple complex and inter–related IT project tasks that often require managing teams of contractor personnel at multiple locations. Provides overall direction of program activities. Manages and maintains contractor interface with the senior levels of the customer's organization. Consults with customer and contractor personnel to formulate and review task plans and deliverables, ensuring conformance with program and project task schedules and costs and contractual obligations. Establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, oversees the successful completion of all assigned tasks, and assumes the initiative and provides support to marketing personnel in identifying and acquiring potential business. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Program Manager, IT, Level I	Bachelor's degree in related discipline and/or related and applicable IT certifications.	14
Program Manager, IT, Level II	Master's degree in related discipline and/or related and applicable IT certifications.	16
Program Manager, IT, Level III	Master's degree in related discipline and/or related and applicable IT certifications.	20

PROGRAM MANAGER, CYBER		
Serves as the program manager typically responsible for organizing, directing, and managing all aspects of contract operational support functions involving multiple complex and inter–related cyberspace operations projects/tasks that often require managing teams of contractor personnel at multiple locations. Provides overall direction of program activities. Manages and maintains contractor interface with the senior levels of the customer's organization. Consults with customer and contractor personnel to formulate and review task plans and deliverables, ensuring conformance with program and project task schedules and costs and contractual obligations. Establishes and maintains technical and financial reports to show progress of projects to management and customers, organizes and assigns responsibilities to subordinates, oversees the successful completion of all assigned tasks, and assumes the initiative and provides support to marketing personnel in identifying and acquiring potential business. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Program Manager, Cyber, Level I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Program Manager, Cyber, Level II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Program Manager, Cyber, Level III	Master's degree in related discipline and/or related and applicable cyber certifications.	20

RISK AND VULNERABILITY ANALYST		
Supports the identification, assessment, prioritization, and management of risks and vulnerabilities followed by the coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. Supports all aspects of the Risk Management Framework to include categorize, select, implement, assess, authorize, and monitor security controls. Supports the systematic examination of information systems and networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	MINIMUM EDUCATION/CERTIFICATION LEVEL	MINIMUM YEARS OF EXPERIENCE
Risk and Vulnerability Analyst, Associate, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Risk and Vulnerability Analyst, Intermediate, Level II	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	3–6
Risk and Vulnerability Analyst, Senior, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Risk and Vulnerability Analyst, Principal, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Risk and Vulnerability Analyst, Sr. Principal, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12
Risk and Vulnerability Analyst, Subject Matter Expert I	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	14
Risk and Vulnerability Analyst, Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16
Risk and Vulnerability Analyst, Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20
Risk and Vulnerability, Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	14
Risk and Vulnerability, Sr. Manager	Master's degree in related discipline and/or related and applicable cyber certifications.	16

Risk and Vulnerability, Director	Master’s degree in related discipline and/or related and applicable cyber certifications.	20

SENIOR ANALYST/ENGINEER		
Performs a variety of software/programming related functions which are broad in nature and are concerned with execution of Feasibility Studies, Joint Test and Evaluations, Test and Evaluations, and Quick Reaction Tests. Provides technical solutions to a wide range of difficult problems related to task order requirements and must have ability to provide solutions that are imaginative, thorough and practicable, and consistent with organization objectives. Discipline supports analysis, design or maintenance of complex software systems, including computer simulation, client/server architectures, networking techniques ad protocols, databases, programming languages, and/or operating systems. Work is reviewed upon completion for adequacy in meeting objectives. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Senior Analyst/Engineer, Level I	Associate's degree in related discipline and/or related and applicable cyber certifications.	0–3
Senior Analyst/Engineer, Level II	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	3–6
Senior Analyst/Engineer, Level III	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	6–10
Senior Analyst/Engineer, Level IV	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	10
Senior Analyst/Engineer, Level V	Bachelor's degree in related discipline and/or related and applicable cyber certifications.	12

SUBJECT MATTER EXPERT I		
Provides technical knowledge and analysis of highly specialized applications and operational environment, high–level functional systems analysis, design, integration, documentation and implementation advice on moderately complex problems that require an appropriate level of knowledge of the subject matter for effective implementation. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions. Assists other senior consultants with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture, networking; telecommunications, automation; communications protocols, risk management/electronic analysis, software; lifecycle management, software development methodologies, and modeling and simulation. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Subject Matter Expert I	Bachelor’s degree in related discipline and/or related and applicable cyber certifications.	14

SUBJECT MATTER EXPERT II		
Analyzes user needs to determine functional requirements and define problems and develop plans and requirements in the subject matter area for moderately complex to complex systems related to information systems architecture, networking; telecommunications, automation, communications protocols, risk management/electronic analysis, software, lifecycle management, software development methodologies, and modeling and simulation. Performs functional allocation to identify required tasks and their interrelationships. Identify resources required for each task. Possess requisite knowledge and expertise so recognized in the professional community that the government is able to qualify the individual as an expert in the field for an actual task order. Demonstrates exceptional oral and written communication skills. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Subject Matter Expert II	Master's degree in related discipline and/or related and applicable cyber certifications.	16

SUBJECT MATTER EXPERT III		
Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development, and implementation for complex to extremely complex systems in the subject matter area. Makes recommendations and advise on organization–wide system improvements, optimization or maintenance efforts in the following specialties: information systems architecture; networking; telecommunications; automation; communications protocols; risk management/electronic analysis; software; lifecycle management; software development methodologies; and modeling and simulation. Commensurate experience in IT and in new and related older technology that directly relates to the required area of expertise. Labor Category may require a Security Clearance		
SERVICE PROPOSED LABOR CATEGORY	**MINIMUM EDUCATION/CERTIFICATION LEVEL**	**MINIMUM YEARS OF EXPERIENCE**
Subject Matter Expert III	Master's degree in related discipline and/or related and applicable cyber certifications.	20